Form PTO-1449 (MODIFIED)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. 068398-0102	SERIAL NO. 09/761,771
INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*		APPLICANT Virgil D. Gligor et al.	
		FILING DATE 01/18/2001	GROUP ART UNIT Unassigned

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

m	A1	A.J. Menezes et al, "Hash Functions and Data Integrity", Handbook of Applied Crytography, Chp 7, pp 223-282; Chp 9, pp 321-383, 1997; CRC Press, Boca Raton
m	A2	Gligor et al, "Object Migration and Authentication", IEEE Transactions on Software Engineering SE-5, vol. 5, pp. 607-611, 1979, IEEE
m	A3	NBS FIPS Pub 46, titled "Data Encryption Standard", National Bureau of Standards, U.S. Dept of Commerce January 1977, pp. 1-18
m	A4	NBS FIPS Pub 81, Titled "DES Modes of Operation", National Bureau of Standards, U.S. Dept of Commerce pp. 1-17, December 1980
m	A5	Meyer et al, Cryptography; A New Dimension in Computer Data Security", A Guide For The Design and Implementation of Secure Systems, pp. 69-71, 1982, John Wiley & Sons, 2nd printing
m	A6	Bellare et al, "A Concrete Security Treatment of Symmetric Encryption", Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, 1997, pp. 394-403
m	A7	C.M. Campbell, "Design and Specification of Cryptographic Capabilities", in Computer Science And The Data Encryption Standard, (D.K. Brandstad (ed.) National Bureau of Standards Special Publications 500-527 U. S. Dept of Commerce, February 1978, pp. 54-66
m	A8	Naor et al, "From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions From MACs", in Advances in Cryptolog – CRYPTO '98 (LNCS 1462), pp. 267-282, 1998, Springer-Verlag
m	A9	Goldwasser et al, "Lecture Notes on Cryptography", 1999, Available at http://www.cse.ucsd.edu/users/mihir/papers/gb.pdf
m	A10	Kohl et al, RFC 1510, The Kerberos Network Authentication Service (V5)", Internet Request For Comments 1510

EXAMINER	DATE CONSIDERED
m	12/7/04

* **EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.**

July 17, 2001

Form PTO-1449 (MODIFIED)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. 068398-0102	SERIAL NO. 09/761,771
INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*		APPLICANT Virgil D. Gligor et al.	
		FILING DATE 01/18/2001	GROUP ART UNIT Unassigned

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

m	A11	Petrank et al, "CBC MAC for Real-Time Data Sources:, Manuscript Available at http://www.cs.technion.ac.il/~erez/publications.html, 1999
m	A12	Jueneman et al, "Message Authentication with Manipulation Detection Codes", Proc. Of the IEEE Symp. on Security and Privacy, Oakland, CA, pp. 33-54, 1983, IEEE Computer Society
m	A13	Stubblebine et al, "On Message Integrity in Cryptographic Protocols", Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 85-104, 1992, IEEE Computer Society Press
m	A14	Kohl et al, "The use of Encryption in Kerberos for Network Authentication", Advances in Cryptology-CRYPTO 1989, (LNCS 435), pp. 35-43, 1990, Digital Equip. Corp.
m	A15	D. E. Knuth, "The Art of Computer Programming – Volume 2: Seminumerical Algorithms", 1981, (2nd ed.) Chapter 3, pp. 1-110, Addison-Wesley

EXAMINER	DATE CONSIDERED
m	12/7/04

* **EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.**

July 17, 2001

Form PTO-1449 (MODIFIED)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. 068398-0102	SERIAL NO. 09/761,771
INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*		APPLICANT Virgil D. Gligor et al.	
		FILING DATE 01/18/2001	GROUP ART UNIT 2131

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB-CLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

m	A1	Gligor Virgil D. and Donescu Pompiliu. "Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes." VDG Inc. 27 October 2000. Pages 1 – 30. <http://citeseer.nj.nec.com/cs>.
m	A2	Rogaway, Phillip. "Comments to NIST Concerning AES Modes of Operation: PMAC: A Parallelizable Message Authentication Code." Univ. of CA at Davis and Chiang Mai Univ. Thailand. 16 October 2000. Pages 1 – 6. http://citeseer.nj.nec.com/cs>.
m	A3	Proceedings IEEE Symposium on Security and Privacy. Jueneman, R.R., Matyas, S.M., and Meyer, C.H. "Message Authentication with Manipulation Detection Codes." Pages 33 – 54. 25 April 1983.

EXAMINER	DATE CONSIDERED
m	12/7/04

* **EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.**